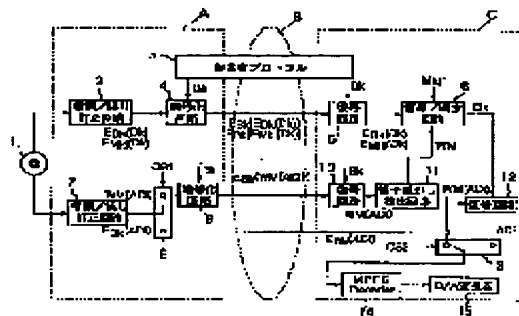


(11)Publication number : 11-232779
(43)Date of publication of application : 27.08.1999

(21)Application number : 10-323879
(22)Date of filing : 13.11.1998

(30)Priority
Priority number : 09361980 Priority date : 20.11.1997 Priority country : JP

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent illegal copy of multi-media data recorded in an information recording medium by using electronic watermark information and key information.
SOLUTION: Electronic watermark information WMXAdi incorporated in multi-media data ADi is extracted in an electronic watermark extracting circuit 11 of a decoding unit C side. And a disk key Dk is obtained by using this electronic watermark information WM and a partial master key Mkj". And multi-media data ADi is decoded by using this obtained disk key.



[Date of request for examination]	06.02.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-232779

(43) 公開日 平成11年(1999) 8月27日

(51) Int.Cl.⁸
 G 1 1 B 20/10
 G 0 6 F 12/14
 G 0 9 C 1/00
 5/00

識別記号
 3 2 0
 6 3 0
 6 6 0

F I
 G 1 1 B 20/10
 G 0 6 F 12/14
 G 0 9 C 1/00
 5/00

H
 3 2 0 B
 6 3 0 C
 6 6 0 D

審査請求 未請求 請求項の数 4 O L (全 20 頁) 最終頁に続く

(21) 出願番号 特願平10-323879

(22) 出願日 平成10年(1998)11月13日

(31) 優先権主張番号 特願平9-361980

(32) 優先日 平9(1997)11月20日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 加藤 拓

東京都府中市東芝町1番地 株式会社東芝
府中工場内

(72) 発明者 加藤 岳久

東京都府中市東芝町1番地 株式会社東芝
府中工場内

(72) 発明者 遠藤 直樹

東京都府中市東芝町1番地 株式会社東芝
府中工場内

(74) 代理人 弁理士 鈴江 武彦 (外6名)

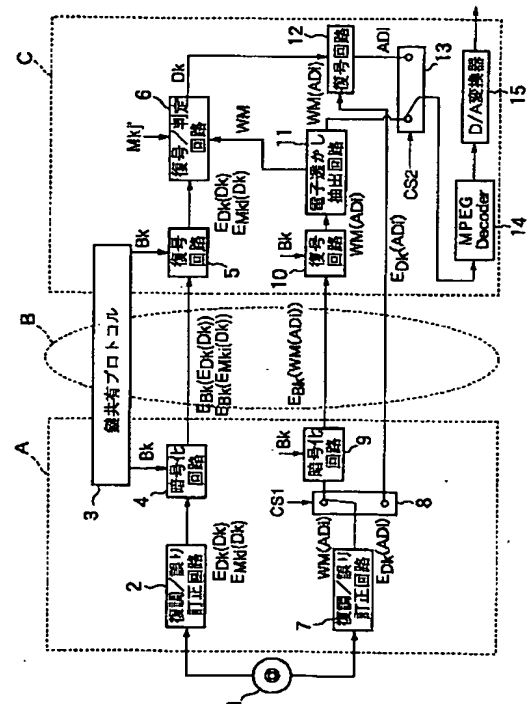
最終頁に続く

(54) 【発明の名称】 コピー防止装置

(57) 【要約】

【課題】 本発明は、電子透かし情報と、鍵情報とを使用することにより、情報記録媒体に記録されたマルチメディアデータの不正コピーを防止する。

【解決手段】 マルチメディアデータADiに埋め込まれた電子透かし情報WM×ADiは、復号ユニットC側の電子透かし抽出回路11において抽出される。そして、この電子透かし情報WMと、部分マスター鍵Mkj'を使用してディスク鍵Dkを得る。そして、この得られたディスク鍵を使用して、マルチメディアデータADiを復号する。



【特許請求の範囲】

【請求項1】 暗号化ユニットと、

CPUバスを介して前記暗号化ユニットに接続された復号化ユニットとを具備し、

前記暗号化ユニットは、

ディスク鍵自身を使用して暗号化された暗号化ディスク鍵を、前記暗号化ユニットと前記復号化ユニットとの間で共有されている共有暗号化鍵を使用して暗号化する第1の暗号化手段と、

前記第1の暗号化手段により暗号化されたディスク鍵を前記CPUバスを介して送信する第1の送信手段と、

マスター鍵を使用して暗号化されたディスク鍵を前記共有暗号化鍵を使用して暗号化する第2の暗号化手段と、

前記第2の暗号化手段により暗号化されたディスク鍵を前記CPUバスを介して送信する第2の送信手段と、

前記マスター鍵の一部である電子透かし情報が埋め込まれたマルチメディアデータを前記共有暗号化鍵を使用して暗号化する第3の暗号化手段と、

前記第3の暗号化手段により暗号化されたマルチメディアデータを前記CPUバスを介して送信する第3の送信手段と、

前記ディスク鍵を使用して暗号化されたマルチメディアデータを送信する第4の送信手段とを具備し、

前記復号化ユニットは、

前記第1の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第1の復号手段と、

前記第2の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第2の復号手段と、

前記第3の送信手段から送信されたマルチメディアデータを前記共有暗号化鍵を使用して復号する第3の復号手段と、

前記第3の復号化手段により復号されたマルチメディアデータから前記透かし情報を抽出する抽出手段と、

前記第1の復号手段により復号されたディスク鍵と、前記第2の復号手段により復号されたディスク鍵と、前記抽出手段により抽出された透かし情報と、前記マスター鍵の一部に対応する部分マスター鍵とに基づいて、ディスク鍵を取得するディスク鍵取得手段と、

前記ディスク鍵取得手段により取得されたディスク鍵を使用して、前記第4の送信手段により送信されたマルチメディアデータを復号する第4の復号手段とを具備することを特徴とするコピー防止装置。

【請求項2】 前記ディスク鍵取得手段は、

前記部分マスター鍵と前記透かし情報とに基づいて、マスター鍵候補を取得する第1の取得手段と、

前記第1の取得手段により取得されたマスター鍵候補を使用して、前記第2の復号手段により復号されたディスク鍵を復号することにより第1のディスク鍵候補を取得する第2の取得手段と、

前記第2の取得手段により取得された第1のディスク鍵

候補を使用して、前記第1の復号手段により復号されたディスク鍵を復号することにより第2のディスク鍵候補を取得する第3の取得手段と、

前記第2の取得手段により取得された第1のディスク鍵候補と、前記第3の取得手段により取得された第2のディスク鍵候補とが一致しているか否かを判定する判定手段と、

前記判定手段により前記第1のディスク鍵候補と前記第2のディスク鍵候補とが一致している判定された場合に、

前記第1のディスク鍵候補をディスク鍵と決定する決定手段とを具備することを特徴とする請求項1記載のコピー防止装置。

【請求項3】 暗号化ユニットと、

CPUバスを介して前記暗号化ユニットに接続された復号化ユニットとを具備し、

前記暗号化ユニットは、

ディスク鍵自身を使用して暗号化された暗号化ディスク鍵を、前記暗号化ユニットと前記復号化ユニットとの間で共有されている共有暗号化鍵を使用して暗号化する第1の暗号化手段と、

前記第1の暗号化手段により暗号化されたディスク鍵を前記CPUバスを介して送信する第1の送信手段と、

マスター鍵を使用して暗号化されたディスク鍵を前記共有暗号化鍵を使用して暗号化する第2の暗号化手段と、

前記第2の暗号化手段により暗号化されたディスク鍵を前記CPUバスを介して送信する第2の送信手段と、

前記ディスク鍵で暗号化され、前記マスター鍵の一部である電子透かし情報が埋め込まれたマルチメディアデータを前記CPUバスを介して送信する第3の送信手段と、

前記ディスク鍵及び前記透かし情報を使用して暗号化されたマルチメディアデータを送信する第4の送信手段とを具備し、

前記復号化ユニットは、

前記第1の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第1の復号手段と、

前記第2の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第2の復号手段と、

前記第1の復号手段により復号されたディスク鍵と、前記第2の復号手段により復号されたディスク鍵と、前記

マスター鍵の一部に対応する部分マスター鍵とに基づいて、ディスク鍵を取得するディスク鍵取得手段と、

前記ディスク鍵取得手段により取得されたディスク鍵を使用して、前記第3の送信手段により送信されたマルチメディアデータを復号する第3の復号手段と、

前記第3の復号手段により復号されたマルチメディアデータから電子透かし情報を抽出する抽出手段と、

前記抽出手段により抽出された電子透かし情報と、前記ディスク鍵取得手段により取得されたディスク鍵とに基づいて、前記第4の送信手段により送信されたマルチメ

ディアデータを復号する第4の復号手段とを具備することを特徴とするコピー防止装置。

【請求項4】 暗号化ユニットと、
CPUバスを介して前記暗号化ユニットに接続された復号化ユニットとを具備し、
前記暗号化ユニットは、
ディスク鍵自身を使用して暗号化された暗号化ディスク鍵を、前記暗号化ユニットと前記復号化ユニットとの間で共有されている共有暗号化鍵を使用して暗号化する第1の暗号化手段と、
前記第1の暗号化手段により暗号化されたディスク鍵を前記CPUバスを介して送信する第1の送信手段と、
マスター鍵を使用して暗号化されたディスク鍵を前記共有暗号化鍵を使用して暗号化する第2の暗号化手段と、
前記第2の暗号化手段により暗号化されたディスク鍵を前記CPUバスを介して送信する第2の送信手段と、
前記ディスク鍵で暗号化され、前記マスター鍵の一部である電子透かし情報が埋め込まれたマルチメディアデータを前記CPUバスを介して送信する第3の送信手段と、
前記ディスク鍵で暗号化され、前記電子透かし情報が重畳されたマルチメディアデータを前記CPUバスを介して送信する第4の送信手段と、
前記復号化ユニットは、
前記第1の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第1の復号手段と、
前記第2の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第2の復号手段と、
前記第1の復号手段により復号されたディスク鍵と、前記第2の復号手段により復号されたディスク鍵と、前記マスター鍵の一部に対応する部分マスター鍵とに基づいて、ディスク鍵を取得するディスク鍵取得手段と、
前記ディスク鍵取得手段により取得されたディスク鍵を使用して、前記第3の送信手段により送信されたマルチメディアデータを復号する第3の復号手段と、
前記第3の復号手段により復号されたマルチメディアデータから電子透かし情報を抽出する抽出手段と、
前記ディスク鍵取得手段により取得されたディスク鍵を使用して、前記第4の送信手段により送信されたマルチメディアデータを復号する第4の復号手段と、
前記抽出手段により抽出された電子透かし情報を使用して、前記第4の復号手段により復号されたマルチメディアデータを復号する第5の復号手段とを具備することを特徴とするコピー防止装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデジタル記録されたデータに対して記録媒体からの不正なコピーを防止するためのコピー防止装置に関する。

【0002】

【従来の技術】従来、デジタル化されたマルチメディア情報（画像、音声など）の記録媒体としては、フロッピーディスク、コンパクトディスク、DVD（デジタルビデオディスク）などが開発されている。

【0003】上記のような様々のデジタル記録媒体において、通常デジタルデータはそのまま（圧縮や符号化され復号可能なものも含む）記録されるため、記録されたデータは他の媒体に劣化することなく容易にコピー可能であり、著作権侵害などの問題が発生している。

【0004】この問題を解決するために、デジタルデータを暗号化して記録媒体に記録する方法も存在するが、この場合にも記録したデータの暗号化に用いた暗号化鍵の管理に不備があるとコピーが可能となってしまう。

【0005】

【発明が解決しようとする課題】本発明は、上記事情を考慮してなされたもので、デジタル記録された記録媒体からの不正なコピーを防止するためのコピー防止装置を提供することを目的とする。

【0006】

【課題を解決するための手段】したがって、まず、本発明の第1の発明によれば、暗号化ユニットと、CPUバスを介して前記暗号化ユニットに接続された復号化ユニットとを具備し、前記暗号化ユニットは、ディスク鍵自身を使用して暗号化された暗号化ディスク鍵を、前記暗号化ユニットと前記復号化ユニットとの間で共有されている共有暗号化鍵を使用して暗号化する第1の暗号化手段と、前記第1の暗号化手段により暗号化されたディスク鍵を前記CPUバスを介して送信する第1の送信手段と、マスター鍵を使用して暗号化されたディスク鍵を前記共有暗号化鍵を使用して暗号化する第2の暗号化手段と、前記第2の暗号化手段により暗号化されたディスク鍵を前記CPUバスを介して送信する第2の送信手段と、前記マスター鍵の一部である電子透かし情報が埋め込まれたマルチメディアデータを前記共有暗号化鍵を使用して暗号化する第3の暗号化手段と、前記第3の暗号化手段により暗号化されたマルチメディアデータを前記CPUバスを介して送信する第3の送信手段と、前記ディスク鍵を使用して暗号化されたマルチメディアデータを送信する第4の送信手段とを具備し、前記復号化ユニットは、前記第1の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第1の復号手段と、前記第2の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第2の復号手段と、前記第3の送信手段から送信されたマルチメディアデータを前記共有暗号化鍵を使用して復号する第3の復号手段と、前記第3の復号化手段により復号されたマルチメディアデータから前記透かし情報を抽出する抽出手段と、前記第1の復号手段により復号されたディスク鍵と、前記第2の復号手段により復号されたディスク鍵と、前記

抽出手段により抽出された透かし情報と、前記マスター鍵の一部に対応する部分マスター鍵とに基づいて、ディスク鍵を取得するディスク鍵取得手段と、前記ディスク鍵取得手段により取得されたディスク鍵を使用して、前記第4の送信手段により送信されたマルチメディアデータを復号する第4の復号手段とを具備することを特徴とするコピー防止装置である。

【0007】また、本発明の第2の発明によれば、第1の発明において、前記ディスク鍵取得手段は、前記部分マスター鍵と前記透かし情報とに基づいて、マスター鍵候補を取得する第1の取得手段と、前記第1の取得手段により取得されたマスター鍵候補を使用して、前記第2の復号手段により復号されたディスク鍵を復号することにより第1のディスク鍵候補を取得する第2の取得手段と、前記第2の取得手段により取得された第1のディスク鍵候補を使用して、前記第1の復号手段により復号されたディスク鍵を復号することにより第2のディスク鍵候補を取得する第3の取得手段と、前記第2の取得手段により取得された第1のディスク鍵候補と、前記第3の取得手段により取得された第2のディスク鍵候補とが一致しているか否かを判定する判定手段と、前記判定手段により前記第1のディスク鍵候補と前記第2のディスク鍵候補とが一致している判定された場合に、前記第1のディスク鍵候補をディスク鍵と決定する決定手段とを具備することを特徴とするコピー防止装置である。

【0008】さらに、本発明の第3の発明によれば、暗号化ユニットと、CPUバスを介して前記暗号化ユニットに接続された復号化ユニットとを具備し、前記暗号化ユニットは、ディスク鍵自身を使用して暗号化された暗号化ディスク鍵を、前記暗号化ユニットと前記復号化ユニットとの間で共有されている共有暗号化鍵を使用して暗号化する第1の暗号化手段と、前記第1の暗号化手段により暗号化されたディスク鍵を前記CPUバスを介して送信する第1の送信手段と、マスター鍵を使用して暗号化されたディスク鍵を前記共有暗号化鍵を使用して暗号化する第2の暗号化手段と、前記第2の暗号化手段により暗号化されたディスク鍵を前記CPUバス介して送信する第2の送信手段と、前記ディスク鍵で暗号化され、前記マスター鍵の一部である電子透かし情報が埋め込まれたマルチメディアデータを前記CPUバスを介して送信する第3の送信手段と、前記ディスク鍵及び前記透かし情報を使用して暗号化されたマルチメディアデータを送信する第4の送信手段とを具備し、前記復号化ユニットは、前記第1の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第1の復号手段と、前記第2の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第2の復号手段と、前記第1の復号手段により復号されたディスク鍵と、前記第2の復号手段により復号されたディスク鍵と、前記マスター鍵の一部に対応する部分マスター鍵と

に基づいて、ディスク鍵を取得するディスク鍵取得手段と、前記ディスク鍵取得手段により取得されたディスク鍵を使用して、前記第3の送信手段により送信されたマルチメディアデータを復号する第3の復号手段と、前記第3の復号手段により復号されたマルチメディアデータから電子透かし情報を抽出する抽出手段と、前記抽出手段により抽出された電子透かし情報と、前記ディスク鍵取得手段により取得されたディスク鍵とに基づいて、前記第4の送信手段により送信されたマルチメディアデータを復号する第4の復号手段とを具備することを特徴とするコピー防止装置である。

【0009】さらに、本発明の第4の発明によれば、暗号化ユニットと、CPUバスを介して前記暗号化ユニットに接続された復号化ユニットとを具備し、前記暗号化ユニットは、ディスク鍵自身を使用して暗号化された暗号化ディスク鍵を、前記暗号化ユニットと前記復号化ユニットとの間で共有されている共有暗号化鍵を使用して暗号化する第1の暗号化手段と、前記第1の暗号化手段により暗号化されたディスク鍵を前記CPUバスを介して送信する第1の送信手段と、マスター鍵を使用して暗号化されたディスク鍵を前記共有暗号化鍵を使用して暗号化する第2の暗号化手段と、前記第2の暗号化手段により暗号化されたディスク鍵を前記CPUバス介して送信する第2の送信手段と、前記ディスク鍵で暗号化され、前記マスター鍵の一部である電子透かし情報が埋め込まれたマルチメディアデータを前記CPUバスを介して送信する第3の送信手段と、前記ディスク鍵で暗号化され、前記電子透かし情報が重畳されたマルチメディアデータを前記CPUバスを介して送信する第4の送信手段と、前記復号化ユニットは、前記第1の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第1の復号手段と、前記第2の送信手段から送信されたディスク鍵を前記共有暗号化鍵を使用して復号する第2の復号手段と、前記第1の復号手段により復号されたディスク鍵と、前記第2の復号手段により復号されたディスク鍵と、前記マスター鍵の一部に対応する部分マスター鍵とに基づいて、ディスク鍵を取得するディスク鍵取得手段と、前記ディスク鍵取得手段により取得されたディスク鍵を使用して、前記第3の送信手段により送信されたマルチメディアデータを復号する第3の復号手段と、前記第3の復号手段により復号されたマルチメディアデータから電子透かし情報を抽出する抽出手段と、前記ディスク鍵取得手段により取得されたディスク鍵を使用して、前記第4の送信手段により送信されたマルチメディアデータを復号する第4の復号手段と、前記抽出手段により抽出された電子透かし情報を使用して、前記第4の復号手段により復号されたマルチメディアデータを復号する第5の復号手段とを具備することを特徴とするコピー防止装置である。

【0010】

【発明の実施の形態】本実施形態では、あるデータ a を鍵 K を用いて暗号化する操作を $E_k(a)$ と表現し、あるデータ a を鍵 K を用いて復号する操作を $D_k(a)$ と表現する。この表現を用いることによって、例えばあるデータ a を鍵 K を用いて暗号化し、それを復号する操作は、 $D_k(E_k(a))$ と表される。

【0011】本実施形態では、DVD に記録された、MPEG-Audioというデータ圧縮規格に従って圧縮され、暗号化された音声データを再生するシステムを例にとって説明する。

【0012】本実施形態では、例えば、予め定められた複数個のマスター鍵を用意し、その内の1つまたは複数のマスター鍵が、復号ユニットメーカ（あるいはDVD の制作・販売会社）などに所定の単位ごとに割り当てられていることを前提とする。

＜第1の実施の形態＞以下、本発明の第1の実施形態について説明する。

【0013】図1は、本発明の第1の実施の形態に係るコピー防止装置を示すブロック図である。

【0014】本実施形態に係るシステムは、パーソナル・コンピュータ（以下PCと略す）などの計算機内に備えられた再生に用いるCPUのいわゆるCPU BUS に接続されるものであり、暗号化されたデータがCPU BUS 上を流れる構成を有するものである。なお、図1では、再生に用いるCPU に関する部分のみを示している。

【0015】図1に示すように、本実施の形態のコピー防止装置は、暗号化ユニットA及び復号ユニットCを備えている。この暗号化ユニットA及び復号ユニットCは、DVD 1からデータを読み出すDVD 駆動装置に設けられても良い。また、DVD 駆動装置にCPUバスを介さずに接続されてもよい。

【0016】暗号化ユニットAと復号ユニットCとは、CPU BUS Bに接続されている。復号ユニットCからのデータの出力は、CPU BUS B以外の例えばI/O ポート等を通じて行われる。つまり、本実施形態では、データの入出力はCPU BUS Bを介さずに行われるが、暗号化ユニットAと復号ユニットCとの間でのデータ転送には、CPU BUS Bが用いられる。

【0017】暗号化ユニットAは、復調／誤り訂正回路2、7、暗号化回路4、9および制御スイッチ8を備えている。制御スイッチ8には、データ列の最初の処理単位が入力された場合には暗号化回路9にデータを渡し、それ以外の場合にはそのままCPU BUS Bに出力するような制御信号(CSI)が入力される。

【0018】図1においては、暗号化ユニットA内には、2つの暗号化回路4、9を図示しているが、実際には1つの暗号化回路で実現可能である。ここでは、暗号化ユニットAは独立した1つのICチップとして形成されるものとする。

【0019】一方、復号ユニットCは、復号回路5、1

0、12、マスター鍵復号／判定回路6、電子透かし抽出回路11及び制御スイッチ13を備えている。

【0020】また、制御スイッチ13には、データ列の最初の処理単位が入力される場合には電子透かし抽出回路11からの信号を入力信号とし、それ以外の場合には復号回路12からの信号を入力信号とするような制御信号(CS2)が入力される。

【0021】さらに、復号ユニットC内には、MPEG-Decoder 14および復号された音声データをデジタルデータからアナログデータに変換するD/A変換器15を備えている。

【0022】同図においては、復号ユニットC内には、4つの復号回路5、10、12、14を示しているが、実際には1つの復号回路で実現可能である。復号ユニットCは、独立した1つのICチップとして形成されるものとする。

【0023】また、復号ユニットC内には、後述するマスター鍵の一部が登録され（作り込まれ）ている。マスター鍵は利用者が外部から取得できない様に、復号ユニットCのチップにおいて利用者が意図的に取り出せない様にチップ内部の秘匿された領域に記録されているものとする。

【0024】ここで、DVD 1に記録する、ディスク鍵をマスター鍵 M_{ki} を用いて暗号化して生成された $EM_{ki}(D_k)$ の種類数と、復号ユニットC内に持つ部分マスター鍵の M_{kj}' の種類数の設定については、例えば、次に示すように幾つかの方法が考えられる。

【0025】（方法1） DVD 1には、 i を $1 \sim n$ のいずれかとする1つのマスター鍵によって暗号化されたディスク鍵 $EM_{ki}(D_k)$ を記録し、復号ユニットC内には、 $j=1 \sim n$ の全てに対応する n 個の部分マスター鍵 M_{kj}' を備える。

【0026】（方法2） DVD 1には、 $i=1 \sim n$ の全てに対応する n 個のマスター鍵によって暗号化されたディスク鍵 $EM_{ki}(D_k)$ を記録し、復号ユニットC内には、 j が $1 \sim n$ のいずれか1つの部分マスター鍵 M_{kj}' を備える。

【0027】（方法3） 上記（方法2）を拡張したもので、DVD 1には $i=1 \sim n$ の全てに対応する n 個のマスター鍵によって暗号化されたディスク鍵 $EM_{ki}(D_k)$ を記録し、復号ユニットC内には、 j を $1 \sim n$ の内から予め選択された m ($2 < m < n$) 個の部分マスター鍵 M_{kj}' を備える。

【0028】（方法4） 上記（方法3）においてDVD 1と復号ユニットCを逆にした例で、DVD 1には i を $1 \sim n$ の内から予め選択された m ($2 < m < n$) 種類のものとする m

個のマスター鍵で暗号化されたディスク鍵 $EM_{ki}(D_k)$ を記録し、復号ユニットC内には $j=1 \sim n$ の全てに対応する n 個の部分マスター鍵 M_{kj}' を備える。

【0029】（方法5） DVD 1には $i=1 \sim n$ の全てに対応する n 個のマスター鍵で暗号化されたディスク鍵 $EM_{ki}(D_k)$ を記録し、復号ユニットC内にも $j=1 \sim n$ の全てに

対応する n 個の部分マスター鍵 Mk_j' を備える。

【0030】また、電子透かしとして埋め込まれる一部の鍵情報 WM および復号／判定回路6内の演算も上記の方法によって変更される。

【0031】なお、CPU BUS Bを介して行われる暗号通信に用いられる暗号化鍵／復号鍵は、共通鍵暗号 Bk とする。この暗号化ユニットAと復号ユニットC間の暗号化鍵の共有の方法は、従来の方法と同様とする。

【0032】さらに、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該計算機のCPUで実行することにより実現することができる。この制御部による制御の具体例としては、DVD1からのデータの読み出しに関する指示、データ伝送先の指定、復号ユニットからのデータ出力に関する指示等である。

【0033】また、この制御部のトリガーは、例えば、ユーザ・インタフェースを介してユーザにより行われる場合と、あるアプリケーションプログラム中のプロセスからかけられる場合などが考えられる。

【0034】本実施形態では、デジタル元音声データ系列をD-Audio、音声データ列(圧縮されたデータ列)を $AD=\{AD1, AD2, \dots, ADi, \dots\}$ 、マスター鍵の一部のデータが電子透かしとして埋め込まれた音声データを $WM(ADi)$ で表す。

【0035】音声データ列 AD には場合によって、ここで埋め込まれる電子透かし情報とは別に、コピー制御用の電子透かし情報が埋め込まれていることもある。さらに、暗号化ユニットと復号ユニット間で共有した暗号鍵(以下共有暗号化鍵)を Bk 、音声データ列を暗号化する暗号化鍵(ディスク鍵)を Dk 、ディスクキーを暗号化するための n 個の暗号化鍵(マスター鍵)の鍵束を $\{Mk1, Mk2, \dots, Mk_i, \dots, Mkn\}$ 、復号ユニットに登録されている部分マスター鍵の鍵束を $\{Mk1', Mk2', \dots, Mk_j, \dots, Mkm'\}$ とする。

【0036】なお、部分マスター鍵とは n 個のマスター鍵の中の m 個の鍵に対応する鍵であり、1つ1つの部分マスター鍵は $WM(ADi)$ から抽出されたデータとの間である種の演算を行うことによってマスター鍵が求められるように予め用意されたデータである。

【0037】 $EDk(Dk)$ はディスク鍵自身を用いて暗号化して生成されたディスク鍵を示し、 $\{EMki(Dk) (i=1, \dots, n)\}$ は n 個のマスター鍵をそれぞれ用いて暗号化して生成されたディスク鍵を示し、 $WM(ADi)$ は電子透かし技術を用いてマスター鍵の一部のデータを埋め込んで生成された音声データ ADi を示し、 $EDk(ADi)$ はディスク鍵 Dk を用いて暗号化して生成された音声データを示し、 $EBk(EDk(Dk))$ は共有暗号化鍵 Bk を用いて暗号化して生成されたディスク鍵を用いて暗号化されたディスク鍵自身を示し、 $EBk(EMki(Dk))$ は共有暗号化鍵 Bk を用いて暗号化して生成されたマスター鍵束を用いて暗号化されたディスク鍵を示し、 $EBk(EDk(ADi))$ は共有暗号化鍵 Bk を用

いて暗号化して生成されたディスク鍵を用いて暗号化された音声データをそれぞれ表す。

【0038】DVD1上では、ディスク鍵をディスク鍵自身で暗号化して生成された $EDk(Dk)$ およびディスク鍵をマスター鍵束で暗号化して生成された $\{EMki(Dk)\}$ は、最内周部の鍵記録領域(リードインエリア)に、音声データ列 $AD=\{AD1, MD2, \dots, ADi, \dots\}$ の内でマスター鍵情報の一部を電子透かしとして埋め込まれた $WM(ADi)$ およびディスク鍵を用いて暗号化して生成された $EDk(ADi)$ は、データ記録領域(データエリア)に記録されているものとする。

【0039】以下、図2のフローチャートを参照しながら、本実施形態の動作について説明する。

【0040】ステップS11で、既存の暗号化鍵共有プロトコル3を用いて、暗号化ユニットAと復号ユニットCとの間の通信に使用する暗号化鍵 Bk を両ユニットで共有する。

【0041】ステップS12で、図示しないDVD駆動装置によりDVD1に記録されている、ディスク鍵 Dk 自身を用いて暗号化されたディスク鍵 $EDk(Dk)$ 、マスター鍵束を用いて暗号化されたディスク鍵 $\{EMki(Dk)\}$ を読み込み、暗号化回路4で暗号化共有鍵 Bk を用いて暗号化し、 $EBk(EDk(Dk))$ 、 $\{EBk(EMki(Dk))\}$ を生成し、CPU Interface Bを通じて復号ユニットCに送る。なお、DVD1から読み出されたデータは、暗号化回路4に入力される前に、復調／誤り訂正回路2によって復調およびデータ中の誤り訂正が行われる。

【0042】ステップS13で、復号ユニットCでは、復号回路5において、CPU Interface Bを介して受け取った $EBk(EDk(Dk))$ 、 $\{EBk(EMki(Dk))\}$ を暗号化共有鍵 Bk を用いて復号し、 $EDk(Dk)$ 、 $\{EMki(DK)\}$ を得る。

【0043】ステップS14で、暗号化ユニットAでは、図示しないDVD駆動装置によりDVD1に記録されている、マスター鍵 Mki の一部の情報を電子透かしとして埋め込まれた音声データ $WM(ADi)$ を読み込み、暗号化回路9で暗号化共有鍵 Bk を用いて暗号化し、 $EBk(WM(ADi))$ を生成し、CPU Interface Bを通じて復号ユニットCに送る。なお、DVD1から読み出されたデータは、暗号化回路9に入る前に、復調／誤り訂正回路7によって復調およびデータ中の誤り訂正が行われる。

【0044】ステップS15で、復号ユニットCでは、復号回路10において、CPU Interface Bを通じて受け取った $EBk(WM(ADi))$ を暗号化共有鍵 Bk を用いて復号し、 $WM(ADi)$ を取り出した上で、電子透かし抽出回路11においてデータ ADi に埋め込まれたマスター鍵 Mki の一部の情報 WM を抽出する。なお、情報 WM を抽出後は、 $WM(ADi)$ は、制御スイッチ13を介してそのままMPEG-Decoder14に送られる。

【0045】ステップS16で、ステップS13およびステップS15でそれぞれ得られたディスク鍵 Dk 自身を

用いて暗号化されたディスク鍵EDk (Dk) 、マスター鍵束を用いて暗号化されたディスク鍵 {EMki (Dk)} およびマスター鍵の一部情報WM、さらに復号ユニットに予め登録されている部分マスター鍵束を用いて、復号／判定回路6においてディスク鍵Dkが取り出される。

【0046】以下、図3を参照して、復号／判定回路6内の動作を説明する。

【0047】復号ユニットC内にある部分マスター鍵束 {Mkj'} の登録されたメモリ (J0) から部分マスター鍵Mkj' を取り出し、マスター鍵の一部情報WMを用いて、予め定められたマスター鍵を生成するための演算 (J1) を施し、マスター鍵候補Mkj を得る。

【0048】復号回路J2では、マスター鍵束 {Mki} を用いて暗号化されたディスク鍵EMki (Dk) にマスター鍵候補Mkj を用いて復号処理を施し、ディスク鍵候補Dk' を得る。復号回路J3では、ディスク鍵自身を用いてディスク鍵を暗号化したEDk (Dk) に、ディスク鍵候補Dk' を用いて復号処理を施し、ディスク鍵候補Dk'' を得る。

【0049】J4では、ディスク鍵候補Dk'' とディスク鍵候補Dk' とを比較し、同じであればディスク鍵候補Dk' を正しいディスク鍵Dkとして復号／判定回路6から送り出す。異なっていた場合には、正しいディスク鍵Dkが得られるまで以上の操作を繰り返す行う。

【0050】ステップS17で、図示しないDVD 駆動装置によりDVD 1に記録されている、ディスク鍵Dkで暗号化された音声データEDk (ADi) を読み出し、CPU Interface Bを介して復号ユニットCに送る。なお、DVD 1から読み出されたデータは、CPUInterface Bに送り出される前に、復調／誤り訂正回路7によって復調およびデータ中の誤り訂正が行われる。

【0051】ステップS18で、復号ユニットCでは、復号回路12において、CPU BUS Bを通じて受け取ったEDk (ADi) を、ディスク鍵Dkを用いて復号し、平文 (plaintext) である圧縮された音声データADi を得ることが出来る。

【0052】ステップS19で、さらに復号処理を続けるかどうかの判断を行い、続ける場合にはステップS17およびステップS18の処理が繰り返す行われる。

【0053】以上のようにして得られた音声データADi は、例えばMPEG-Audioというデータ圧縮規格に従って圧縮されている場合には、MPEG-Decoder 14で復号 (伸長) され、そしてD/A 変換器15でアナログ信号に変換された後、図示しないスピーカーアンプなどの音声増幅／出力装置に送られ、再生される。

【0054】なお、上記ステップS12とステップS14はどちらを先に実行しても構わない。

【0055】また、マスター鍵の一部情報を電子透かし情報として埋め込まれる音声データは、マスター鍵の一部鍵情報を埋め込むのに十分な長さがあるものとし、もし長さが足りない場合には、電子透かし情報は、複数の

音声データ単位に渡って埋め込まれる。

【0056】復号回路12からMPEG-Decoder 14に音声データADi を渡す際には、1つの音声データADi 単位ごとに渡すだけでなく、所定数の単位で渡しても良い。

【0057】したがって、本実施の形態のコピー防止装置によれば、ディスク鍵を復号するのに電子透かし情報を使用しなければならないことから、不正にコピーされたメディアを販売するという不法な行為を防止することができ、著作権侵害を防止することができる。

【0058】また、本実施形態のコピー防止装置によれば、暗号化および復号に用いる回路は、図1から解るようにDVD 1などのデジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、例えば暗号や電子透かしが破られたとしても、復号ユニットC (あるいは暗号化ユニットAおよび復号ユニットC) を交換するだけで良い。

【0059】本発明のコピー防止装置によれば、CPU BUS Bを流れるデータを保存したとしても、データには暗号化処理及び電子透かし処理が施されているので、当該データを再生または利用することが出来ない。

【0060】さらに、復号ユニットC側に予め登録されるマスター鍵情報を完全な鍵情報とはせず、DVD 1の再生のたびに、コンテンツに含まれる鍵情報を用いなければ完全な鍵情報を得ることが出来ないようになっていたため、万が一復号ユニット内に登録されたマスター鍵情報が完全に露呈し、それを元に不正利用を試みた場合でも、DVD 1 を正常に再生することが出来ない。

【0061】最後に、本実施形態における、DVD 1への音声データおよび鍵情報の記録方法について図4を用いて説明する。

【0062】本システムでは、入力音声アナログデータ (A-Audio) の場合には、まず、A/D変換器21でデジタルデータ (D-Audio) に変換し、この変換されたデジタルデータに電子透かし埋め込み回路22において、必要に応じてコピー制御 (CCI) などの情報を埋め込む。なお、電子透かし埋め込み回路22は場合によって省略可能である。その上で、MPEG-Audio符号化回路23によってデータが圧縮される。

【0063】このMPEG-Audio符号化回路23の出力音声データADi は、切り替えスイッチ24において、マスター鍵の一部情報WMを埋め込む場合には電子透かし埋め込み回路25へ出力される。

【0064】電子透かし埋め込み回路25では、データが入力された場合には、マスター鍵の一部情報を電子透かしとして音声データADi に埋め込んだ上で、データWM (ADi) を出力する。

【0065】この電子透かし埋め込み回路25には、予め用意されたマスター鍵の一部情報WMが全て埋め込まれるまで音声データADi が入力される。そして、マスター鍵の一部情報WMが埋め込まれた音声データWM (ADi) はそ

のままDVD 27 に記録される。

【0066】また、マスター鍵の一部情報WMを埋め込む必要の無い音声データADi は、切り替えスイッチ24によって、暗号化回路26へ出力される。暗号化回路26では、入力された音声データADi をディスク鍵Dkを用いて暗号化する。暗号化された音声データDk(ADi) は、DVD 27に記録される。

【0067】さらに、DVD 27には、音声データADi を暗号化する際に使用したディスク鍵Dkをマスター鍵束で暗号化した{EMki(Dk)}およびディスク鍵を用いてディスク鍵自身で暗号化したDk(Dk)が記録される。

【0068】なお、図4の例では、マスター鍵の一部情報をMPEG-Audio符号化回路23によって圧縮された音声データADi に電子透かしとして埋め込んでいるが、電子透かし埋め込み回路25において圧縮前のデジタル音声データに埋め込むことも可能である。その場合には、電子透かし埋め込み回路25は省略できる。

<第2の実施の形態>次に、本発明の第2の実施の形態に係るコピー防止装置について説明する。

【0069】図5は、本発明の第2の実施の形態に係るコピー防止装置を示す図である。なお、図1と同一部分には、同一符号を付し、その説明を省略する。

【0070】本実施形態に係るコピー防止装置は、パーソナル・コンピュータなどの計算機内に備えられた再生に用いるCPUのいわゆるCPU BUS に接続されるものであり、暗号化されたデータがCPU BUS 上を流れる構成を有するものである。なお、図5では、再生に用いるCPU に関する部分のみを示している。

【0071】暗号化ユニットAと復号ユニットCとは、CPU BUS Bに接続されている。復号ユニットからのデータの出力は、CPU BUS 以外の例えばI/O ポート等を通じて行われる。つまり、本実施形態では、第1の実施の形態と同様に、データの入出力はCPU BUS Bを介さずに行われるが、暗号化ユニットAと復号ユニットCとの間でのデータ転送には、CPU BUS Bが用いられる。

【0072】暗号化ユニットAは、復調/誤り訂正回路2、7、暗号化回路4を備えている。暗号化ユニットAは、独立した1つのICチップとして形成されるものとする。

【0073】一方、復号ユニットCは、復号回路5、34、マスター鍵復号/判定回路31、電子透かし抽出回路35、制御スイッチ33 および鍵生成回路32を備えている。

【0074】制御スイッチ33には、データ列の最初の処理単位が入力される場合にはディスク鍵Dkを入力信号とし、それ以外の場合には鍵生成回路32からの信号を入力信号とするような制御信号(CS)が別に入力される。

【0075】また、本実施形態では、復号ユニットC内にMPEG-Decoder 14および復号された音声データをデジタルデータからアナログデータに変換するD/A変換

器15を備えているものとする。

【0076】図5においては、復号ユニットC内には2つの復号回路5、34を示しているが、実際には1つの復号回路で実現可能である。復号ユニットCは、独立した1つのICチップとして形成されるものとする。

【0077】また、復号ユニット内には後述するマスター鍵の一部が登録され(作り込まれ)ている。マスター鍵は利用者が外部から取得できない様に、復号ユニットのチップにおいて利用者が意図的に取り出せない様にチップ内部の秘匿された領域に記録されているものとする。

【0078】ここで、DVD 1に記録する、ディスク鍵をマスター鍵Mki を用いて暗号化して生成されたEMki(Dk)の種類数と、復号ユニットC内に持つ部分マスター鍵のMki の種類数の設定については、第1の実施形態の場合と同様に考えることができる。

【0079】なお、CPU BUS Bを介して行われる暗号通信に用いられる暗号化鍵/復号鍵(共通鍵暗号を利用するため共にBk)は、暗号化ユニットAと復号ユニットCとの間で共有されるものとする。

【0080】さらに、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該計算機のCPU で実行することにより実現することができる。この制御部による制御の具体例としては、DVD からのデータの読み出しに関する指示、データ伝送先の指定、復号ユニットからのデータ出力に関する指示等である。

【0081】また、この制御部のトリガーは、例えば、ユーザ・インタフェースを介してユーザにより行われる場合と、あるアプリケーションプログラム中のプロセスからかけられる場合などが考えられる。

【0082】本実施形態では、デジタル元音声データ系列をD-Audio、音声データ列(圧縮されたデータ列)をAD={AD1, AD2, ..., ADi, ...}、マスター鍵の一部のデータが電子透かしとして埋め込まれた音声データをWM(ADi)で表す。

【0083】音声データ列ADには、場合によって、ここで埋め込まれる電子透かし情報とは別に、コピー制御用の電子透かし情報が埋め込まれていることもある。さらに、暗号化ユニットAと復号ユニットCとの間で共有した暗号鍵(以下共有暗号化鍵)をBk、音声データ列を暗号化する暗号化鍵(ディスク鍵)をDk、ディスクキーを暗号化するためのn個の暗号化鍵(マスター鍵)の鍵束を{Mk1, Mk2, ..., Mki, ..., Mkn}、復号ユニットに登録されているマスター鍵の鍵束を{Mk1, Mk2, ..., Mkj, ..., Mkm}とする。

【0084】図5において、EDk(Dk)はディスク鍵自身を用いて暗号化して生成されたディスク鍵を示し、{EMki(Dk) (i=0, 1, ..., n-1)}はn個のマスター鍵をそれぞれ用いて暗号化して生成されたディスク鍵を示し、WM(A Di)は電子透かし技術を用いて以降の音声データの暗号

化鍵を生成するために必要な情報を埋め込んで生成された音声データを示し、 $E_{Dk+WM}(ADi)$ は事前に電子透かしによって復号ユニットに送った情報WMとディスク鍵Dkを用いて暗号化して生成された音声データを示し、 $EBk(EDk(Dk))$ は共有暗号化鍵Bkを用いて暗号化して生成されたディスク鍵を用いて暗号化されたディスク鍵自身を示し、 $EBk(EMki(Dk))$ は共有暗号化鍵Bkを用いて暗号化して生成されたマスター鍵束を用いて暗号化されたディスク鍵をそれぞれ表す。

【0085】DVD 1上では、ディスク鍵をディスク鍵自身で暗号化して生成された $EDk(Dk)$ およびディスク鍵をマスター鍵束で暗号化して生成された $\{EMki(Dk)\}$ は、最内周部の鍵記録領域（リードインエリア）に、音声データ列 $AD=\{AD1, AD2, \dots, ADi, \dots\}$ の内で以降の音声データの復号鍵を生成する情報の一部を電子透かしとして埋め込まれた $EDk(WM(ADi))$ およびデータ鍵（ディスク鍵と電子透かしとして復号ユニットに送られる情報WMから生成される鍵）を用いて暗号化して生成された $E_{Dk+WM}(ADi)$ は、データ記録領域（データエリア）に記録されているものとする。

【0086】以下、図6のフローチャートを参照しながら、本実施形態の動作について説明する。

【0087】ステップS21で、既存の暗号化鍵共有プロトコルを用いて、暗号化ユニットAと復号ユニットCとの間の通信に使用する暗号化鍵Bkを両ユニットで共有する。

【0088】ステップS22で、図示しないDVD 駆動装置によりDVD 1に記録されている、ディスク鍵Dk自身を用いて暗号化されたディスク鍵 $EDk(Dk)$ 、マスター鍵束を用いて暗号化されたディスク鍵 $\{EMki(Dk)\}$ を読み込み、暗号化回路4で暗号化共有鍵Bkを用いて暗号化し、 $EBk(EDk(Dk))$ 、 $\{EBk(EMki(Dk))\}$ を生成し、CPU Interface B を通じて復号ユニットCに送る。

【0089】なお、DVD 1から読み出されたデータは、暗号化回路Aに入る前に、復調／誤り訂正回路2によって復調およびデータ中の誤り訂正が行われる。

【0090】ステップS23で、復号ユニットCでは、復号回路5において、CPU Interface Bを通じて受け取った $EBk(EDk(Dk))$ 、 $EBk(EMki(Dk))$ を暗号化共有鍵Bkを用いて復号し、 $EDk(Dk)$ 、 $EMki(Dk)$ を得る。

【0091】ステップS24で、ディスク鍵Dk自身を用いて暗号化されたディスク鍵 $EDk(Dk)$ 、マスター鍵束 Mki を用いて暗号化されたディスク鍵 $\{EMki(Dk)\}$ および復号ユニットに予め登録されているマスター鍵束 Mkj を用いて、復号／判定回路31においてディスク鍵Dkが取り出される。

【0092】次に、復号／判定回路31内の動作を説明する。

【0093】復号ユニット内にあるマスター鍵束 $\{Mkj\}$ の登録されたメモリからマスター鍵 Mkj を取り出し、マ

スター鍵束 $\{Mki\}$ を用いて暗号化されたディスク鍵 $EMki(Dk)$ にマスター鍵候補 Mkj を用いて復号処理を施し、ディスク鍵候補 Dk' を得る。

【0094】ディスク鍵自身を用いてディスク鍵を暗号化した $EDk(Dk)$ に、ディスク鍵候補 Dk' を用いて復号処理を施し、ディスク鍵候補 Dk'' を得る。

【0095】ディスク鍵候補 Dk'' とディスク鍵候補 Dk' とを比較し、同じであればディスク鍵候補 Dk' を正しいディスク鍵として復号／判定回路31から送り出す。異なっていた場合には、正しいディスク鍵が得られるまで以上の操作を繰り返し行う。

【0096】ステップ25で、暗号化ユニットAでは、図示しないDVD 駆動装置によりDVD 1に記録されている、ディスク鍵Dkで暗号化された、以降の音声データの復号鍵を生成するために必要な情報が電子透かしとして埋め込まれた音声データ $EDk(WM(ADi))$ を読み込み、CPU Interface B を通じて復号ユニットCに送る。なお、DVD 1から読み出されたデータは、暗号化回路Aに入る前に、復調／誤り訂正回路7によって復調およびデータ中の誤り訂正が行われる。

【0097】ステップS26で、復号ユニットCでは、復号回路34において、CPU Interface Bを通じて受け取った $EDk(WM(ADi))$ をディスク鍵Dkを用いて復号し、WM(ADi)を取り出した上で、電子透かし抽出回路35においてデータADiに埋め込まれた以降の音声データの復号鍵を生成するために必要な情報WMを抽出する。なお、情報WMを抽出後は、WM(ADi)はそのままMPEG-Decoderに送られる。さらに、鍵生成回路32においては、ディスク鍵Dkと鍵生成情報WMを用いて音声データ用の復号鍵 $Dk+WM$ を生成する。

【0098】この際、予めDVD ディスク1に音声データを記録する際に使われた暗号化鍵に対応する復号鍵（共通鍵暗号の場合には同じ鍵になる）を生成するが、最初の音声データの暗号化／復号に使われるディスク鍵、鍵生成情報WMおよび以降の音声データの暗号化／復号に使われる鍵の間には次に述べる様々な関係を設定することが出来る。本説明では、以降の音声データ（暗号化／復号）鍵を $Dk+WM$ と表している。

【0099】（関係1）ディスク鍵Dkと鍵生成情報WMを何らかの手段によってディスク鍵と同じデータ長に調整したものの排他的論理和を求めたものを、以降の音声データの暗号化鍵とする。

【0100】（関係2）鍵生成情報WMを暗号化鍵としてディスク鍵Dkを暗号化したものを、以降の音声データの暗号化鍵とする。

【0101】ステップS27で、図示しないDVD 駆動装置によりDVD 1に記録されている、音声データ鍵 $Dk+WM$ で暗号化された音声データ $E_{Dk+WM}(ADi)$ を読み出し、CPU Interface 3 を通じて復号ユニットCに送る。なお、DVD 1から読み出されたデータは、CPU Interface Bに

送り出される前に、復調／誤り訂正回路7によって復調およびデータ中の誤り訂正が行われる。

【0102】ステップS28で、復号ユニットCでは、復号回路34において、CPU BUS Bを通じて受け取った E_{Dk+WM} (ADi)を、音声データ鍵 $Dk+WM$ を用いて復号し、平文である圧縮された音声データADiを得ることが出来る。

【0103】ステップS29で、さらに復号処理を続けるかどうかの判断を行い、続ける場合にはステップS27およびステップS28が繰り返行われる。

【0104】以上のようにして得られた音声データADiは、例えばMPEG-Audioというデータ圧縮規格に従って圧縮されている場合には、MPEG-Decoder 14で復号(伸長)され、そしてD/A変換器15でアナログ信号に変換された後、図示しないスピーカアンプなどの音声増幅／出力装置に送られ、再生される。

【0105】また、音声データ鍵の鍵生成情報を電子透かし情報として埋め込まれる音声データは、音声データ鍵の鍵生成情報を埋め込むのに十分な長さがあるものとし、もし長さが足りない場合には、電子透かし情報は、複数の音声データ単位に渡って埋め込まれる。

【0106】復号回路34からMPEG-Decoder 14に音声データADiを渡す際には、1つの音声データADi単位ごとに渡すだけでなく、所定数の単位で渡しても良い。

【0107】したがって、本実施の形態のコピー防止装置によれば、マルチメディアデータに透かし情報を埋め込み、この埋め込まれた透かし情報を使用して、マルチメディアデータを復号するので、不正なコピーが行われたメディアを販売するという不法な行為を防止することができ、著作権侵害を防止することができる。

【0108】また、本実施形態では第1の実施の形態と同様に、暗号化および復号に用いる回路は、図5から解るようにDVDなどのデジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、例えば暗号や電子透かしが破られたとしても、復号ユニットC(あるいは暗号化ユニットAおよび復号ユニットC)を交換するだけで良い。

【0109】最後に、本実施形態における、DVD 1への音声データおよび鍵情報の記録方法について図7を用いて説明する。

【0110】本システムでは、入力音声アナログデータA-Audioの場合には、まずAnalogue-to-Digital変換器でデジタル音声データD-Audioに変換した上で入力されるものとする。

【0111】電子透かし埋め込み回路42では、最初に入力されるデジタルデータD-Audioに、音声データをDVD 47に暗号化して記録する際に用いられる暗号化鍵を生成するために必要な情報WMを電子透かし情報として埋め込んだデータが生成され、そのデータはMPEG-Audio符号化器43において圧縮され、音声データWM(ADi)が出

力される。

【0112】その際、鍵生成回路46では、DVD 47への記録用の暗号化鍵を生成するために必要な情報WMとディスク鍵 Dk とから暗号化鍵 $Dk+WM$ を生成する。

【0113】鍵生成回路46は、ディスク鍵 Dk または鍵情報WMのどちらか一方からでは暗号化鍵 $Dk+WM$ が作成できない構成の限りのにおいて、様々なものが考えられる。

【0114】このMPEG-Audio符号化回路43の出力音声データADiは、暗号化回路44においてディスク鍵 Dk を用いて暗号化され、暗号化された音声データ $EDk(WM(ADi))$ はDVD 47に記録される。

【0115】電子透かし埋め込み回路42において、DVD 47への記録用の暗号化鍵 $Dk+WM$ を生成するために必要な情報WMを全て埋め込み終わると、制御信号CSによって切り替えスイッチ41が切り替えられ、それ以降のデジタルデータD-Audioは、そのままMPEG-Audio符号化回路43に入力され、圧縮された音声データADiが出力される。

【0116】暗号化回路44では、暗号化鍵 $Dk+WM$ を用いて、入力された音声データADiを暗号化して、 $E_{Dk+WM}(ADi)$ を出力する。出力された暗号化データ $E_{Dk+WM}(ADi)$ はDVD 47に記録される。

【0117】さらに、DVD 47には、音声データADiを暗号化する際に使用したディスク鍵 Dk をマスター鍵束で暗号化した $\{EMki(Dk)\}$ およびディスク鍵を用いてディスク鍵自身で暗号化した $Dk(Dk)$ が記録される。

【0118】本実施形態では、説明を簡単にするため、MPBG-Audio符号化器で圧縮された音声データADiを直接、暗号化鍵 $Dk+WM$ で暗号化しているが、例えば以下の様に改良することによってさらに強固にデータを守ることができる。

【0119】(改良法) 鍵生成情報WMを時系列に対して変化する情報 Wmi とし、全ての音声データに電子透かし情報として埋め込んだ上で、DVD 47への記録の際の暗号化鍵も埋め込み情報 Wmi を基に毎回変化させ、暗号化鍵を $Dk+Wmi-l$ とし、DVD 47には暗号化された音声データ $EDk+Wmi-l(WM(ADi))$ を記録する。

<第3の実施の形態>図8は、本発明の第3の実施の形態に係るコピー防止装置を示すブロック図である。なお、図1と同一部分には、同一符号を付し、その説明を省略する。また、図8においては、再生に用いるCPUに関する部分のみを示している。

【0120】本実施形態の形態にかかるコピー防止装置は、DVD 1からデータを読み出すDVD駆動装置(図示せず)、このDVD駆動装置にCPU BUSを介さずに接続またはDVD駆動装置に内蔵された暗号化ユニットA、復号ユニットCを備えている。

【0121】暗号化ユニットAと復号ユニットCは、CPU BUS Bに接続されている。復号ユニットCからのデータの出力は、CPU BUS B以外の例えばI/Oポート等を

通じて行われる。つまり、本実施形態では、データの出力はCPU BUS Bを介さずに行われるが、暗号化ユニットAと復号ユニットCとの間でのデータ転送には、CPU BUS Bが用いられる。

【0122】暗号化ユニットAは、復調／誤り訂正回路2、7、暗号化回路4を備えている。暗号化ユニットは独立した1つのICチップとして形成されるものとする。

【0123】一方、復号ユニットCは、復号回路5、50、マスター鍵復号／判定回路31、電子透かし抽出回路51、重畳情報除去回路53 および遅延回路52を備えている。本実施形態では復号ユニットC内にMPEG-Decoder 14および復号された音声データをデジタルデータからアナログデータに変換するA/D変換器15を備えているものとする。

【0124】復号ユニットC内には2つの復号回路5、50を示しているが、実際には1つの復号回路で実現可能である。復号ユニットは、独立した1つのICチップとして形成されるものとする。

【0125】また、復号ユニット内には第2の実施形態と同様にマスター鍵が登録され（作り込まれ）ている。マスター鍵は利用者が外部から取得できない様に、復号ユニットのチップにおいて利用者が意図的に取り出せない様にチップ内部の秘匿された領域に記録されているものとする。

【0126】ここで、DVD 1に記録する、ディスク鍵をマスター鍵 Mk_i を用いて暗号化して生成された $EMk_i(Dk)$ の種類数と、復号ユニットC内に持つマスター鍵の Mk_i の種類数の設定について、第1の実施形態の場合と同様に考えることができる。

【0127】なお、CPU BUS を介して行われる暗号通信に用いられる暗号化鍵／復号鍵（共通鍵暗号を利用するため共に Bk ）は暗号化ユニットAと復号ユニットCとの間で共有されるものとする。

【0128】さらに、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該計算機のCPUで実行することにより実現することができる。この制御部による制御の具体例としては、DVDからのデータの読み出しに関する指示、データ伝送先の指定、復号ユニットからのデータ出力に関する指示等である。

【0129】また、この制御部のトリガーは、例えば、ユーザ・インタフェースを介してユーザにより行われる場合と、あるアプリケーションプログラム中のプロセスからかけられる場合などが考えられる。

【0130】本実施形態では、デジタル元音声データ系列をD-Audio、音声データ列（圧縮されたデータ列）を $AD=\{AD_1, AD_2, \dots, AD_i, \dots\}$ 、何らかの情報が電子透かしとして埋め込まれた音声データを $WM(AD_i)$ で表す。

【0131】音声データ列 AD には場合によって、ここで埋め込まれる電子透かし情報とは別にコピー制御用の電子透かし情報が埋め込まれていることもある。さらに、

暗号化ユニットAと復号ユニットCとの間で共有した暗号鍵（以下共有暗号化鍵）を Bk 、音声データ列を暗号化する暗号化鍵（ディスク鍵）を Dk 、ディスクキーを暗号化するための n 個の暗号化鍵（マスター鍵）の鍵束を $\{Mk_1, Mk_2, \dots, Mk_i, \dots, Mk_n\}$ 、復号ユニットCに登録されているマスター鍵の鍵束を $\{Mk_1, Mk_2, \dots, Mk_j, \dots, Mk_m\}$ とする。

【0132】図8において、 $EDk(Dk)$ はディスク鍵自身を用いて暗号化して生成されたディスク鍵を示し、 $\{EMk_i(Dk) \ (i=0, 1, \dots, n-1)\}$ は n 個のマスター鍵をそれぞれ用いて暗号化して生成されたディスク鍵を示し、 $WM(AD_i)$ は電子透かし技術を用いて音声データ AD_i に以降の音声データの暗号化鍵を生成するために必要な情報を埋め込んで生成された音声データを示す。

【0133】また、 $EDk(WM(AD_i))$ は、ディスク鍵 Dk を用いて暗号化して生成された $WM(AD_i)$ を示し、 $AD_i \times WM$ は、事前に電子透かしによって復号ユニットに送った情報 WM を重ねた音声データ AD_i を示し、 $EDk(AD_i \times WM)$ は、ディスク鍵 Dk を用いて暗号化して生成された $(AD_i \times WM)$ を示し、 $EBk(EDk(Dk))$ は、共有暗号化鍵 Bk を用いて暗号化して生成された $EDk(Dk)$ を示し、 $EBk(EMk_i(Dk))$ は、共有暗号化鍵 Bk を用いて暗号化して生成された $EMk_i(Dk)$ をそれぞれ表す。但し、 \times は、重畳操作を示し、データを攪乱することを目的とする操作を示す。例えば、適当なスクランブルを施すことを示し、 $AD_i \times WM$ は、適当な WM を使用して AD_i をスクランブルすることを示す。

【0134】DVD 1上では、ディスク鍵をディスク鍵自身で暗号化して生成された $EDk(Dk)$ およびディスク鍵をマスター鍵束で暗号化して生成された $\{EMk_i(Dk)\}$ は、最内周部の鍵記録領域（リードインエリア）に、音声データ列 $AD=\{AD_1, AD_2, \dots, AD_i, \dots\}$ の内で以降の音声データに重畳されている情報を電子透かし WM として埋め込まれた音声データをディスク鍵を用いて暗号化して生成された $EDk(WM(AD_i))$ および電子透かし情報 WM の重畳された音声データをディスク鍵を用いて暗号化して生成された $EDk(AD_i \times WM)$ は、データ記録領域（データエリア）に記録されているものとする。

【0135】以下、図9のフローチャートを参照しながら、本実施形態の動作について説明する。

【0136】ステップS31からステップS35までは、第2の実施形態で説明した図6に示したフローチャートのステップS21からステップS25までと同じである。

【0137】ステップS36で、復号ユニットCでは、復号回路50において、CPU Interface Bを通じて受け取った $EDk(WM(AD_i))$ をディスク鍵 Dk を用いて復号し、 $WM(AD_i)$ を取り出した上で、電子透かし抽出回路51においてデータ AD_i に埋め込まれた以降の音声データに重畳されている情報 WM を抽出する。

【0138】なお、情報 WM を抽出後は、 $WM(AD_i)$ はその

ままたMPEG-Decoder 1 4に送られる。この際、予めDVD ディスク 1 に音声データを記録する際に重畳された情報WM および音声データへの情報WMの重畳方法には、例えば以下のように、様々な関係を設定することが出来る。本説明では、この重畳に用いられる演算を記号‘×’で表している。

【0 1 3 9】（関係 1）重畳情報WMを何らかの手段によって音声データADi と同じデータ長に調整した上で、両データの排他的論理和を施す。

【0 1 4 0】（関係 2）重畳情報WMを暗号化鍵として音声データADi を暗号化する。

【0 1 4 1】ステップS 3 7で、図示しないDVD 駆動装置によりDVD 1 に記録されている、ディスク鍵Dkを用いて透かし情報WMの重畳された音声データを暗号化して生成されたされたEDk (ADi×WM) を読み出し、CPU Interface Bを通じて復号ユニットCに送る。

【0 1 4 2】なお、DVD 1 から読み出されたデータは、CPU Interface Bに送り出される前に、復調／誤り訂正回路 7 によって復調およびデータ中の誤り訂正が行われる。

【0 1 4 3】ステップS 3 8で、復号ユニットCでは、復号回路 5 0において、CPU BUS Bを通じて受け取ったEDk (ADi×WM) を、音声データ鍵Dkを用いて復号し、重畳情報除去回路 5 3において、重畳情報WMを取り除き、平文である圧縮された音声データADi を得る。

【0 1 4 4】ステップS 3 9で、さらに復号処理を続けるかどうかの判断を行い、続ける場合にはステップS 3 7およびステップS 3 8が繰り返される。

【0 1 4 5】以上のようにして得られた音声データADi は、例えばMPEG-Audioというデータ圧縮規格に従って圧縮されている場合には、MPEG-Decoder 1 4で復号（伸長）され、そしてD/A 変換器 1 5でアナログ信号に変換された後、図示しないスピーカーアンプなどの音声増幅／出力装置に送られ、再生される。

【0 1 4 6】また、音声データに埋め込まれる重畳情報は、必要に応じて複数の音声データ単位に渡って埋め込むことも可能である。

【0 1 4 7】復号回路CからMPEG-Decoder 1 4に音声データADi を渡す際には、1つの音声データADi 単位ごとに渡すだけでなく、所定数の単位で渡しても良い。

【0 1 4 8】したがって、本実施の形態のコピー防止装置によれば、電子透かし情報をマルチメディアデータに埋め込み、この埋め込まれた電子透かし情報を使用して、マルチメディアデータを復号するので、不正コピーを防止することができる。

【0 1 4 9】また、本実施形態では上述の実施形態と同様に、暗号化および復号に用いる回路は、図 8 から解るようにDVD などのデジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、例えば暗号や電子透かしが破られたとしても、復号ユニットC（あるい

は暗号化ユニットAおよび復号ユニットC）を交換するだけで良い。

【0 1 5 0】上述のいずれの実施形態も、共有暗号化鍵を使用したCPU BUS 通信部を省略することによって単体のDVD プレーヤーに即した実施形態に直すことが出来る。

【0 1 5 1】最後に、DVD への音声データおよび鍵情報の記録方法について図 1 0 を用いて説明する。

【0 1 5 2】本システムでは、入力音声アナログデータA-Audio の場合には、まず、A/D変換器でデジタル音声データD-Audio に変換した上で入力されるものとする。

【0 1 5 3】電子透かし埋め込み回路 6 4 は、最初に入力されるデジタルデータD-Audioに、以降の音声データに重畳する情報WMを電子透かしとして埋め込み、さらに、MPEG-Audio符号化回路 6 3 で圧縮された上で、電子透かしの埋め込まれた音声情報WM (ADi) が出力される。

【0 1 5 4】暗号化回路 6 2 では、ディスク鍵Dkを用いて電子透かしの埋め込まれた音声情報WM (ADi) を暗号化した音声データEDk (WM (ADi)) が生成される。暗号化された音声データEDk (WM (ADi)) は、DVD 6 1 に記録される。

【0 1 5 5】電子透かし埋め込み回路 6 4 において、音声データに重畳される情報WMを全て埋め込み終わると、制御信号CSによって切り替えスイッチ 6 5 が切り替えられ、それ以降のデジタルデータD-Audio は、MPEG-Audio符号化回路 6 6 で圧縮された後に、電子透かし情報重畳回路 6 7 において、電子透かし情報WMが重畳（ここでは‘×’記号で表記）され、重畳音声データADi×WMが出力される。

【0 1 5 6】重畳音声データADi×WMは、電子透かしの埋め込まれた音声情報WM (ADi) と同様に、暗号化回路 6 2 において、ディスク鍵Dkを用いて暗号化され、暗号化音声データEDk (ADi×WM) としてDVD 6 1 に記録される。

【0 1 5 7】さらに、DVD 6 1 には、音声データADi および重畳音声データADi×WMを暗号化する際に使用したディスク鍵Dkをマスター鍵束で暗号化した{EMKi (Dk)} およびディスク鍵を用いてディスク鍵自身で暗号化したDk (Dk) が記録される。

【0 1 5 8】本実施形態では、説明を簡単にするため、MPEG-Audio符号化器で圧縮された音声データに重畳される情報WMは全データに渡って同じであるが、例えば以下のように改良することによってさらに強固にデータを守ることができる。

【0 1 5 9】（改良法 1）鍵生成情報WMを時系列に対して変化する情報WMi とし、全ての音声データに再生に必要な情報を電子透かし情報として埋め込み、そこで埋め込んだ情報WMi を次の音声データを攪乱する情報とする。つまり、上述の重畳音声データADi×WMは、EDk (WMi (ADi)×WMi-1) の状態でDVD 1 に記録される。

【0160】（改良法 2）鍵生成情報WMを時系列に対して変化する情報W_{Mi}とし、全ての音声データに再生に必要な情報を電子透かし情報として埋め込み、そこで埋め込んだ情報W_{Mi}をそのデータ自身の音声データを攪乱する情報とする。従って、ADiをW_{Mi}で攪乱した上で、さらにそのデータにW_{Mi}を埋め込むことになる。つまり、上述の重畳音声データADi×W_{Mi}は、EDk(W_{Mi}(ADi×W_{Mi}))の状態ではDVD1に記録される。

【0161】（改良法 3）上記改良方法1及び2を一般的に記述することによって、ある時点の音声データに再生に必要な情報を電子透かし情報として埋め込み、そこで埋め込んだ情報W_{Mi}を任意の時点のデータを攪乱する情報とする。従って、ADiをW_{Mj}で攪乱した上で、さらにそのW_{Mj}を他の時点の音声データADjに電子透かしとして埋め込むことになる。つまり、上述の重畳音声データADi×W_{Mj}は、EDk(W_{Mi}(ADi×W_{Mj}))の状態ではDVD1に記録される。

【0162】以上、第1の実施形態、第2の実施形態、第3の実施形態について各々説明してきたが、3つの実施形態をまとめて1つの形態にするなど、本発明はこれらに限定されず種々変形して実施することが出来る。

【0163】各実施形態では、情報の記録媒体をDVDとして説明したが、本発明は、CD-ROM等、他の記録媒体にも適用可能である。

【0164】各実施形態では、復号対象となる情報として音声データを例にとって説明したが、本発明は、画像データなど、他の形態の情報の再生装置等にも適用可能である。

【0165】各実施形態では、復号対象となる情報がMP EG-Audioという規格に従って圧縮されている場合を例にとって説明したが、本発明はこれに限定されず、他の規格によってデータ圧縮あるいは符号化等されていても構わない。この場合、MPEG-Audio復号回路の代わりに、他の対応する復号回路を設ける。また、符号化等されているものであっても構わない。この場合、MPEG-Audio復号回路を除去する。

【0166】また、種々の方式で圧縮等されたデータ（あるいは復号の必要なデータ）のいずれも出力できるように、複数種類の復号回路等を設け、これを適宜切り替えて使用し（あるいはこれらを使用しないように）構成することも可能である。この場合、例えば、DVD等の記録媒体から使用すべき復号回路等を示す識別子を読み込み、この識別子にしたがって適切な復号回路等を選択等する方法が考えられる。

【0167】さらに、第1の実施形態において示した復号／判定回路の構成は一例であり、この他にも種々の構成が考えられる。

【0168】

【発明の効果】本発明によれば、記録データを正しく復号あるいは再現するために必要な情報の一部を、DVD等

の記録媒体に記録されているデータにも電子透かし技術などによって再生に必要な情報を埋め込むことになるため、異なった手段で送られるデータを各々正しく復号（復元）できる正当なもののみが、データを完全に復号（復元）できる。

【0169】この結果、不正にコピーされたメディアを販売するという不法な行為を防止し、著作権をより強固に守ることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るコピー防止装置を示すブロック図

【図2】同実施形態におけるコピー防止装置の動作を示すフローチャート

【図3】同実施形態におけるコピー防止装置のマスター鍵の復号／判定回路の動作を示すフローチャート

【図4】同実施形態におけるコピー防止装置に使用される情報記録媒体へのデータの記録方法を示すブロック図。

【図5】本発明の第2の実施形態に係るコピー防止装置を示すブロック図

【図6】同実施形態のコピー防止装置の動作を示すフローチャート

【図7】同実施形態におけるコピー防止装置に使用される情報記録媒体へのデータの記録方法を示すブロック図。

【図8】本発明の第3の実施形態に係るコピー防止装置を示すブロック図

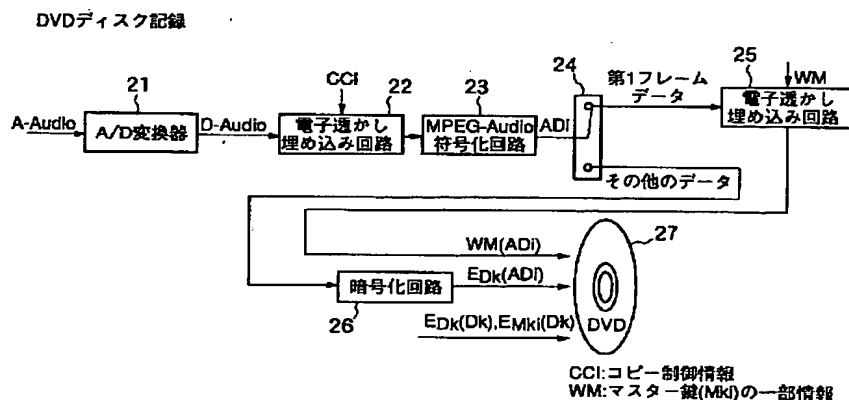
【図9】同実施形態のコピー防止装置の動作を示すフローチャート

【図10】同実施形態におけるコピー防止装置に使用される情報記録媒体へのデータの記録方法を示すブロック図。

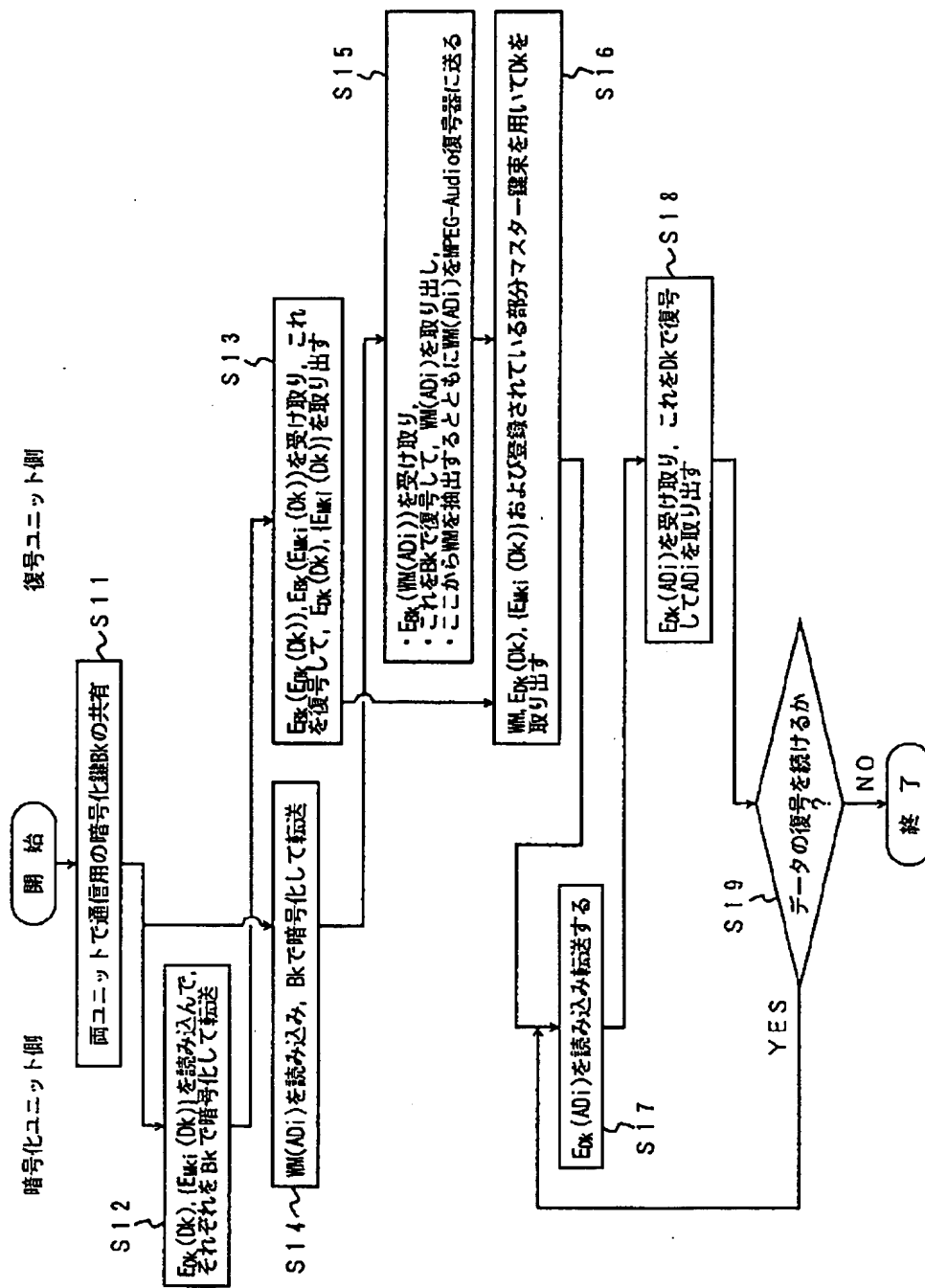
【符号の説明】

- 1…DVD、
- 2…復調／誤り訂正回路、
- 3…鍵共有プロトコル、
- 4…暗号化回路、
- 5…復号回路、
- 6…マスター鍵復号／判定回路、
- 7…復調／誤り訂正回路、
- 8…制御スイッチ、
- 9…暗号化回路、
- 10…復号回路、
- 11…電子透かし抽出回路、
- 12…復号回路、
- 13…制御スイッチ、
- 14…MPEG-Decoder、
- 15…D/A変換器、
- 21…A/D変換器、
- 22…電子透かし埋め込み回路、

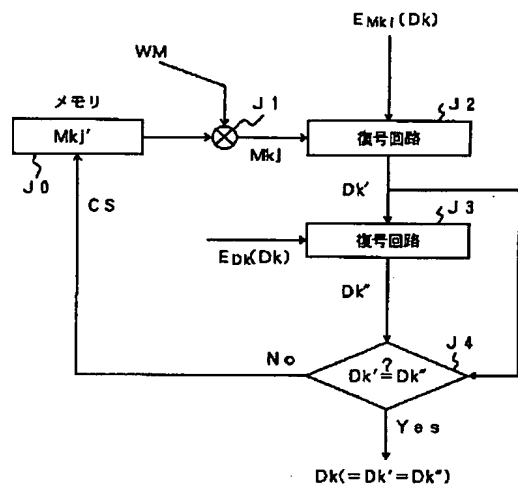
- 【図 1】



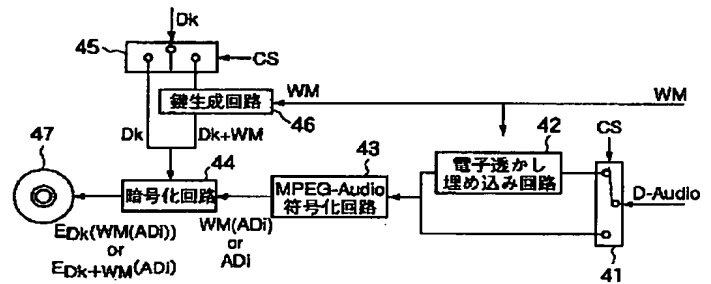
【図2】



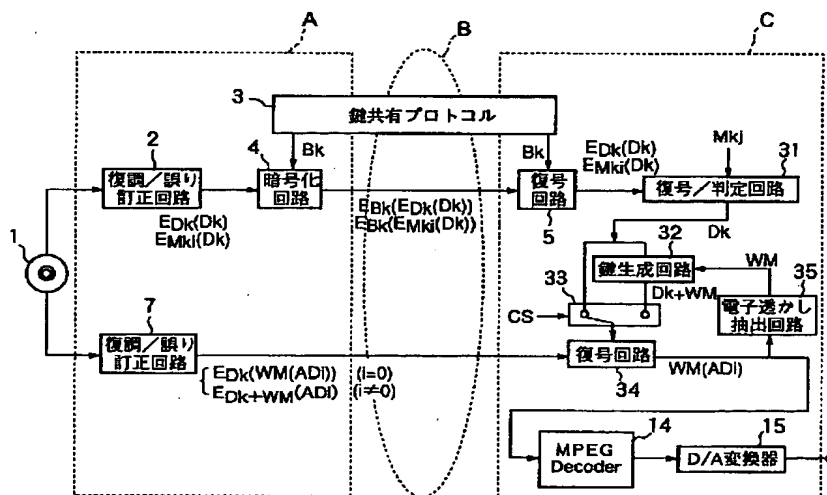
【図3】



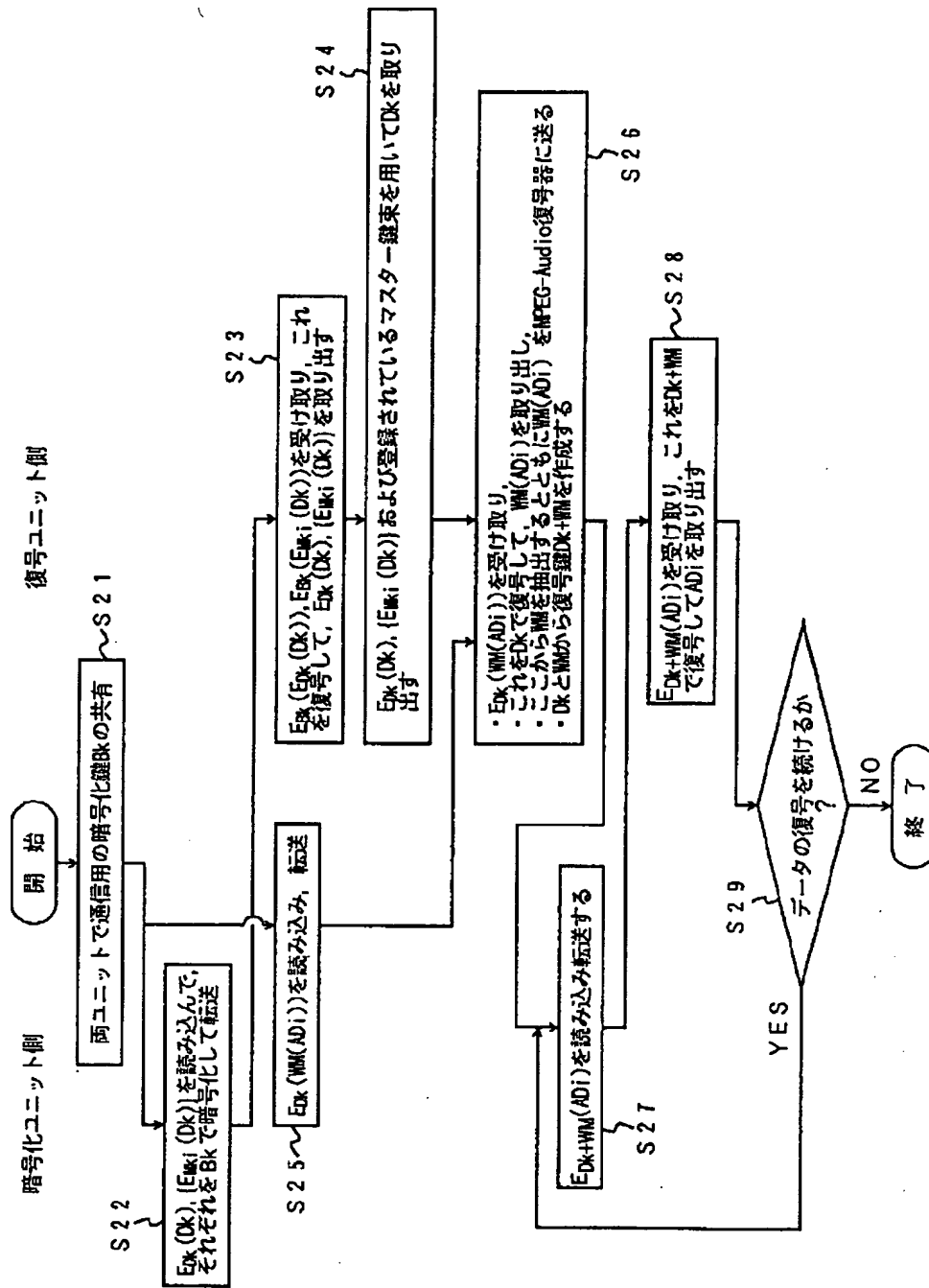
【図7】



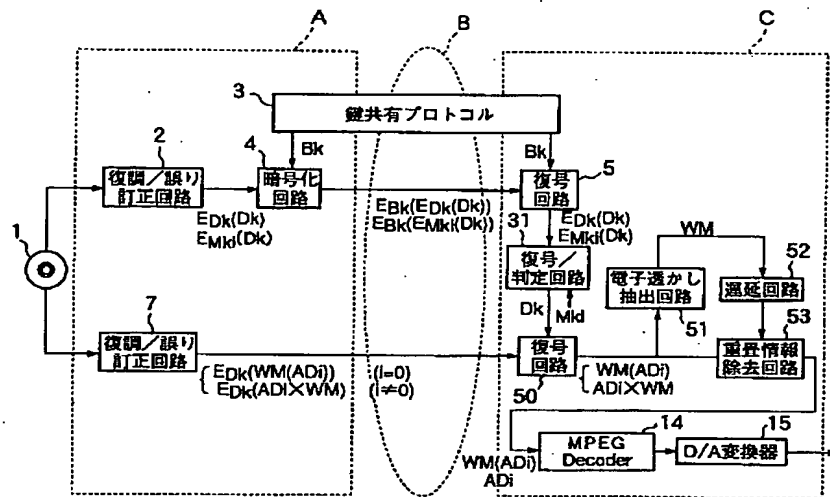
【図5】



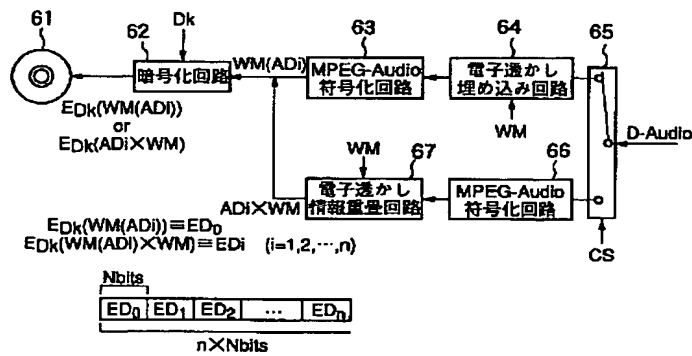
【図6】



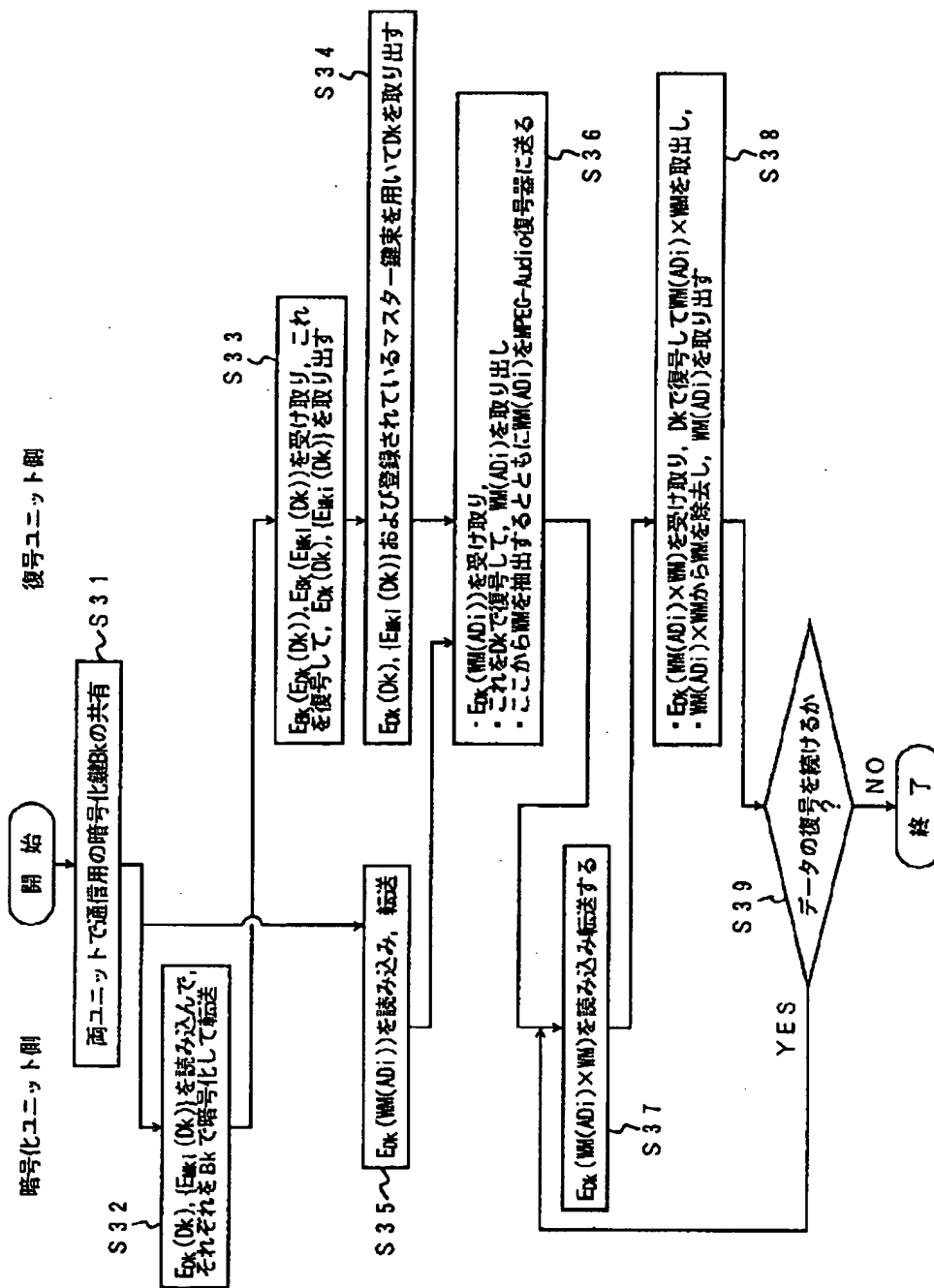
【図8】



【図10】



【図9】



フロントページの続き

(51) Int. Cl. 6

H04L 9/00

識別記号

FI

H04L 9/00

621Z

(72)発明者 山田 尚志
神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内

(72)発明者 遠藤 謙二郎
神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内